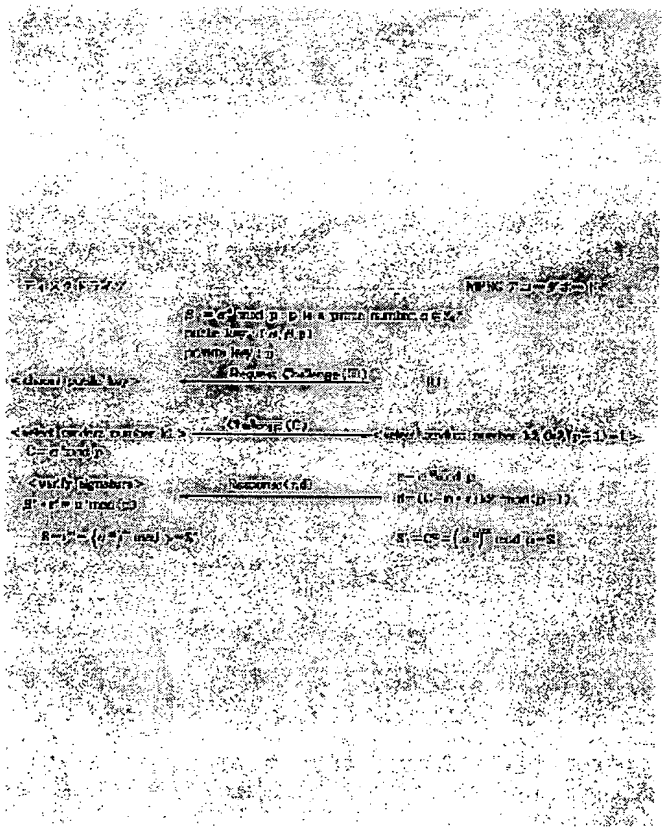
DATA DECODING METHOD AND ITS DEVICE, AUTHENTICATING METHOD, RECORDING MEDIUM, DISK PRODUCING METHOD, RECORDING METHOD AND RECORDING DEVICE

Patent number: JP10065662
Publication date: 1998-03-06
Inventor: ISHIGURO RYUJI; OSAWA YOSHITOMO
Applicant: SONY CORP
Classification:
- international: H04L9/08; G11B20/14; H04L9/14; H04L9/32; H04N7/24
- european:
Application number: JP19970082598 19970401
Priority number(s):

Abstract of **JP10065662**

PROBLEM TO BE SOLVED: To surely prevent illegal copying by ciphering reproduction data which is supplied to a decoder through the use of an undecipherable cipher key.
SOLUTION: When identification data transmitted from an MPEG decoder board and a public key corresponding to its ID are judged to be effective, a disk drive calculates Challenge (C) from an expression C=&alpha k1mod p and supplies it to the MPEG decoder board. In the expression, &alpha and p are the public keys, p is prime number, and k1 is a properly selected random value. The MPEG decoder board selects the random value k2, calculates digital signature r and d and supplies them to the disk drive. The disk drive calculates &beta <r> . &gamma <d> , calculates &alpha <c> mod (p), judges whether or not the both values are equal and calculates Session key (S) in the care of being equal. In the meantime, the decoder board calculates Session key (S'). S becomes the value equal to S' and it means the same cipher key is obtained.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－65662

(43)公開日　平成10年(1998)３月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｃ
Ｇ１１Ｂ	20/14	３４１	9463－5D	Ｇ１１Ｂ	20/14	３４１Ｂ
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６０１Ｅ
	9/32					６４１
Ｈ０４Ｎ	7/24					６７５Ａ

審査請求　未請求　請求項の数23　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願平9－82598

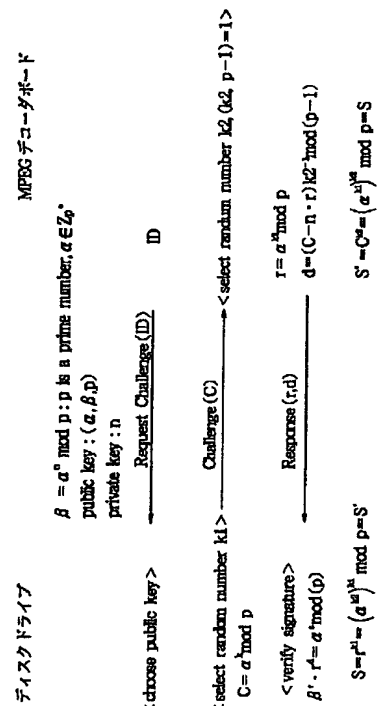
(22)出願日　平成９年(1997)４月１日

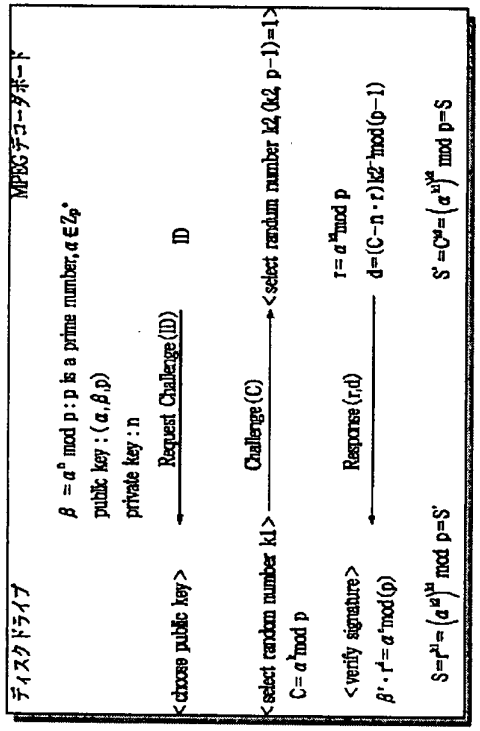
(31)優先権主張番号　特願平8－78647
(32)優先日　平８(1996)４月１日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－147272
(32)優先日　平８(1996)６月10日
(33)優先権主張国　日本（ＪＰ）

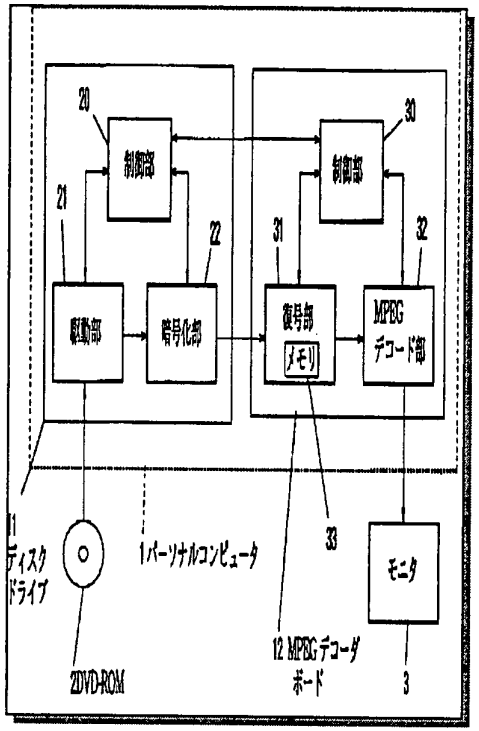
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　弁理士　稲本　義雄

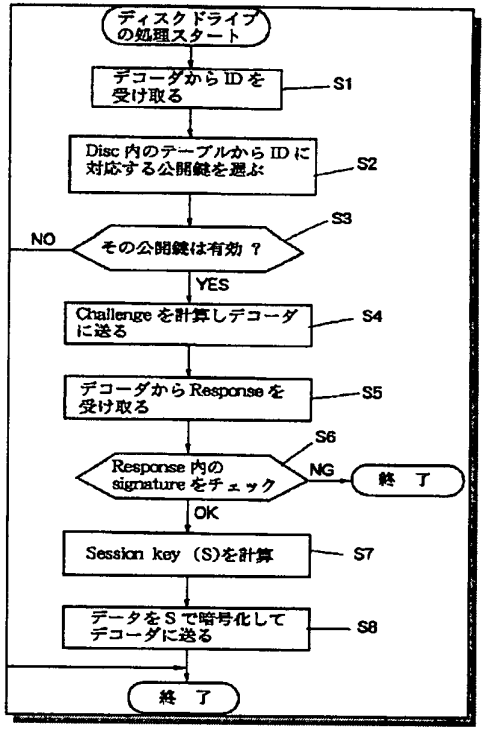
(54)【発明の名称】　データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置

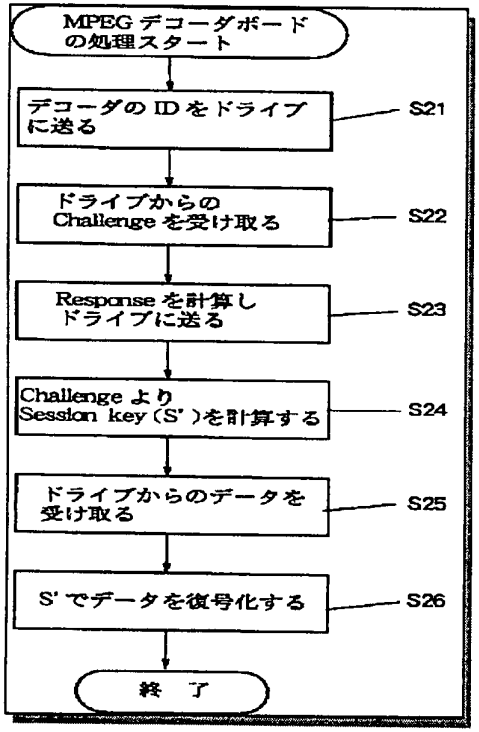
(57)【要約】
【課題】　より安全な復号化方法を実現する。
【解決手段】　ＭＰＥＧデコーダボードは、メモリに記憶されているＩＤをディスクドライブに出力する。ディスクドライブは、ＤＶＤ－ＲＯＭに記憶されているキーテーブルからＩＤに対応する公開鍵を読み出し、この公開鍵を用いて、Ｃｈａｌｌｅｎｇｅ（Ｃ）を演算し、ＭＰＥＧデコーダボードに出力する。ＭＰＥＧデコーダボードは、Ｃｈａｌｌｅｎｇｅ（Ｃ）を用いて、デジタルシグニチャｒ，ｄを演算し、ディスクドライブに出力する。ディスクドライブは、デジタルシグニチャｒ，ｄを用いて、暗号化鍵を演算する。また、ＭＰＥＧデコーダボードは、Ｃｈａｌｌｅｎｇｅ（Ｃ）を用いて、暗号化鍵を演算する。

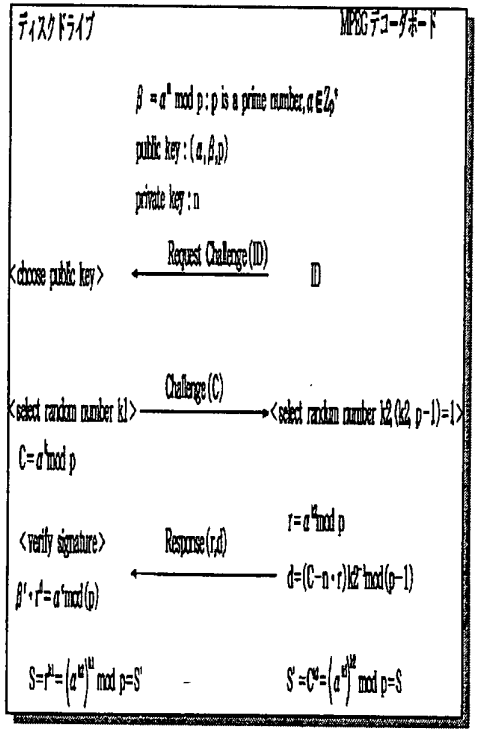


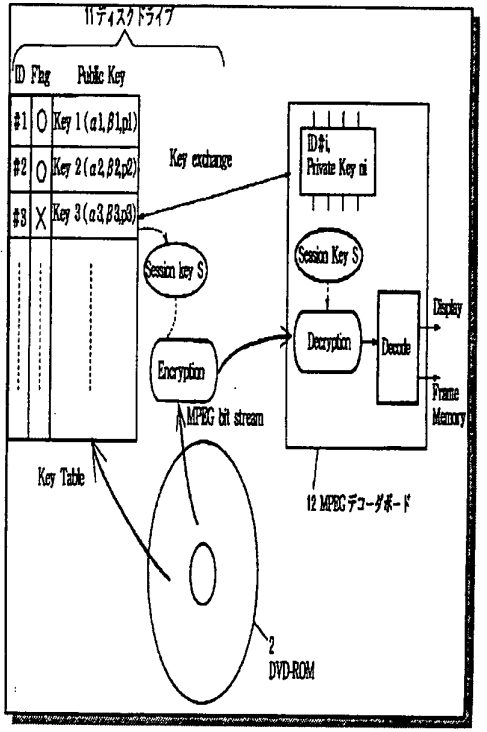

MPEGデコーダボード
ディスクドライブ
β = α^a mod p : p is a prime number, α∈Zp*
public key : (α, β, p)
private key : n
Request Challenge (ID)
ID
<choose public key>
<select random number k1>
C = α^k mod p
Challenge (C)
<select random number k2 (k2, p-1)=1>
r = α^k2 mod p
d = (C - n・r) k2^-1 mod (p-1)
Response (r,d)
<verify signature>
β^r・r^r = α^C mod (p)
S = r^r = (α^a)^k1 mod p = S'
S' = C^a = (α^a)^k2 mod p = S


20
制御部
30
制御部
21
22
31
32
駆動部
暗号化部
復号部
メモリ
MPEG
デコード部
11
ディスク
ドライブ
1パーソナルコンピュータ
33
モニタ
2DVD-ROM
12 MPEGデコーダ
ボード
3


ディスクドライブ
の処理スタート
デコーダからIDを
受け取る
S1
Disc内のテーブルからIDに
対応する公開鍵を選ぶ
S2
その公開鍵は有効？
S3
NO
YES
Challengeを計算しデコーダ
に送る
S4
デコーダからResponseを
受け取る
S5
Response内の
signatureをチェック
S6
NG
終 了
OK
Session key (S)を計算
S7
データをSで暗号化して
デコーダに送る
S8
終 了


MPEGデコーダボード
の処理スタート
デコーダのIDをドライブ
に送る
S21
ドライブからの
Challengeを受け取る
S22
Responseを計算し
ドライブに送る
S23
Challengeより
Session key (S')を計算する
S24
ドライブからのデータを
受け取る
S25
S'でデータを復号化する
S26
終 了


ディスクドライブ
MPEGデコーダボード
β = α^a mod p : p is a prime number, α∈Zp*
public key : (α, β, p)
private key : n
<choose public key>
Request Challenge (ID)
ID
<select random number k1>
Challenge (C)
<select random number k2 (k2, p-1)=1>
C = α^k mod p
r = α^k2 mod p
<verify signature>
Response (r,d)
d = (C - n・r) k2^-1 mod (p-1)
β^r・r^r = α^C mod (p)
S = r^r = (α^a)^k1 mod p = S'
S' = C^a = (α^a)^k2 mod p = S


11ディスクドライブ
ID Flag Public Key
#1 ○ Key 1 (α1, β1, p1)
#2 ○ Key 2 (α2, β2, p2)
#3 × Key 3 (α3, β3, p3)
Key exchange
ID#i
Private Key ni
Session key S
Session Key S
Encryption
Decryption
Decode
Display
Frame Memory
MPEG bit stream
Key Table
12 MPEGデコーダボード
2
DVD-ROM